IDACS NEWS QUARTERLY

IDACS

Special points of interest:

- NCIC Expanded Name Search
- Audit Trails
- BMV Digital Picture Requests
- Misuse of Distribution Codes

Volume 2002 Issue 1

1st Quarter 2002

License Plate Inquiry/Entry—Procedural Change

Files affected: All files that contain a license plate entry. In order to accommodate agencies that are not capable of entering ten (10) characters, NCIC 2000 will search the leftmost eight (8) characters. (The NCIC 2000 format allows for the Vehicle License Plate Number (LIC) Field to contain up to ten (10) characters.

Currently Indiana only allows for eight (8) characters in the Vehicle License Plate Number (LIC) Field. In order to receive a "HIT" response based on an inquiry, the following procedure is to be used.

Entry: If the license plate number exceeds eight (8) characters, the first left eight (8) characters should be entered in the LIC Field with the entire number entered in the Miscellaneous (MIS) Field.

(This will allow for an inquiry using eight (8) characters to match a ten (10) character entry.

Inquiry: Because there are entries in file that were entered using the last eight (8) characters, if a "NOT IN FILE" message is received using the last eight (8) characters, then the first eight (8) characters should be used.

In order to alert agencies that receive a positive vehicle response, a match is not exact to all ten (10) LIC characters, the following caveat will appear at the beginning of the record:

RECORD NIC/ V123456789

IS BASED ON A PARTIAL LIC SEARCH—

VERIFY ALL DATA BEFORE TAKING ACTION BASED ON THIS RESPONSE.

Entry of License Plate Stickers

License Plate Stickers can no longer be entered into the IDACS/ NCIC Article File. When the BMV receives a report of a stolen or lost sticker, a replacement sticker is reissued with the same number that was on the previous sticker which is also the license plate number. This means that the license plate sticker no longer has a unique manufacturer assigned serial number. This information should be disseminated to all dispatch and investigative personnel.

Inside this issue:

NCIC 2000 Expanded Name Search

If the Name and the DOB are specified, primary hits are determined using each input name part as a last name, interchanging the remaining name parts as given names. For example, Bryan, Morgan Lee: - Bryan, Lee Morgan: -Morgan, Lee Bryan: -Morgan, Bryan Lee: - Lee, Morgan Bryan : and Lee, Bryan Morgan.

Also, if the first name is Andrew, Andy will also be searched.

Therefore, if the first name Andrew is used in the inquiry and the entry is made using the first name of Andy a positive response will be returned by NCIC.

040 INDIANA AND III QH INQUIRY

OID/
ATN/ DAVIS,TOM

MKE/QH
ORI/

INQUIRY INFORMATION:

.NAM/ TEST,ANDREW .SEX/M .RAC/W

.DOB/ 12051980 FBI/ MNU/

.SOC/333224444 SID/ PUR/C

NOTE: NAM REQUIRED WHEN USING DOB, SOC, OR MNU.
SEX AND RAC REQUIRED WHEN DOB IS USED.

MSG WAITING

NCIC
12/12/00 1342
INISP0011
DAVIS,TOM
THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR INQUIRY ON NAM/ TEST,ANDREW SEX/M RAC/W DOB/19800805 SOC/333224444 PUR/C

NAME FBI NO. INQUIRY DATE
TEST,ANDY PAUL 111111PB7 2001/12/12
SEX RACE BIRTH DATE HEIGHT WEIGHT EYES HAIR BIRTH PLACE
M W 1980/12/05 508 125 BRO BRO KENTUCKY

FINGERPRINT CLASS PATTERN CLASS
RS WU RS WU RS LS WU WU WU LS
RS WU
ALIAS NAMES
TEST,PAUL

MSG WAITING

The Indiana Criminal History files do not have this capability.

INIII0000
12/12/00 1342
INISP0011

ATN/DAVIS,TOM
THIS INDIANA STATE POLICE CRIMINAL HISTORY RECORD REPONSE IS THE RESULT OF YOUR INQUIRY ON: NAM/TEST, ANDREW

NCIC
12/12/00 1342
INISP0011
DAVIS,TOM

SCARS-MARKS-
TATTOOS SOCIAL SECURITY
SC L LEG 333-22-4444

IDENTIFICATION DATA UPDATED 2001/10/06

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE FOLLOWING:
INDIANA -STATE ID/IN111111

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION INDEX BY USING THE APPROPRIATE
NCIC TRANSACTION.

Planning for the Unexpected. From the Information Security Officer

(ISOTOME 3)

Does your agency have a contingency plan? Your response may be different now, than it would have been before September 11th. A reassessment of resources may be in order to assure that your agency can adequately handle a disaster on a scale you would have previously thought unimaginable. The probability of a natural disaster causing a mission-critical system to become inoperable may still be highly unlikely, but the change of a terrorist attack has grown. Limited staffing may have previously caused your agency to devote resources to other important responsibilities and to assume the risk and the consequences of not developing a contingency plan. However, it does not take a major disaster to disrupt system operations. A simple power outage could cause the loss of data or prevent hundreds of users from accessing important criminal justice information.

"A reassessment of resources may be in order to assure that your agency can adequately handle a disaster on a scale you would have previously thought to be unimaginable"

One of the most important security-related documents that a criminal justice agency should develop and maintain is a contingency plan. A contingency plan provides the procedures that would be followed to ensure the continuity of operations in the event of a system failure. The contingency plan should address the purpose and scope of the project with a clear understanding of the goals and objectives. The authority to implement the plan should be delineated so there is no confusion over who is in charge or who makes the decisions when the time comes. An alternate storage site should be chosen, and the procedures associated with that site should be well documented.

Maintaining officer safety and public safety services should be the ultimate goal in all of the contingency plan segments. A list of hardware and software for the operating system and systems applications should be maintained. System operational techniques, including the telecommunications and firewall profile

A well conceived contingency plan should answer these questions:

1. Are there any agreements with contractors for processing?
2. Are there documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)?
3. What is being backed up?
4. Where are the backup tapes and generations of backups stored?
5. Is there a contingency plan in place for all supporting systems?
6. Are there written procedures posted or easy to locate during an emergency?
7. How often is the contingency plan tested?
8. Have the employees received training in their role relative to the contingency plan?
9. Who should be contacted in the event of a system failure?

The contingency plan should be known to users and tested at least annually. If it is not practical to shut down the entire system, the plan should be tested module while the rest of the system remains in operation. Our best defense is to be prepared for the worst: it can happen.

•

Audit Trails

By CHRISTOPHER YOCHIM, CJIS AUDIT UNIT

In spring 1998, the CJIS Advisory Process members recommended that the FBI director authorize a security management structure to specifically address technical security controls, policy revisions, oversight, training and security incident and notification. In support of this recommendation, the CJIS Audit Unit (CAU) developed technical security elements which were formally incorporated into the biennial National Crime Information Center (NCIC) audit in July 2000 and have been administered at every Control Terminal Agency (CTA) since that time.

The CAU has developed a four-phase technical security audit methodology mirroring that of NCIC Audit. The four phases of the technical security audit are the pre-audit questionnaire, the on-site questionnaire, the audit report and the sanctionable offenses report.

The CAU has developed a four phase technical security audit methodology mirroring that of the NCIC Audit. The four phases of the technical security audit are the pre-audit questionnaire, the on-site audit questionnaire, the audit report, and the sanctionable offenses report. The technical security audit is primarily directed at the CTA. Currently, there is very limited focus at the local level.

The pre-audit questionnaire is sent to the CTA 90 days prior to the NCIC audit and targets such areas as: system design; technical security including authentication, dial-up access, encryption, and Internet access; personnel; training; dissemination; and auditing. The questionnaire was designed to address background and conceptual information regarding the state's CJIS system security design. The questionnaire requests supporting documentation, if available, from the CTA, including system schematics, security policies, implementation plans, security management design prior to the on-site technical audit. It also allows the CTA to conduct a self-review of its own security management design and to identify potential areas for development or improvement.

At the time of the CTA NCIC on-site audit, the auditors meet with the Control Terminal Officer (CTO) or Federal Service Coordinator (FSC), and Information Security Officer (ISO) in order to administer the on-site audit questionnaire. The questionnaire was designed as a follow up to the pre-audit data collection and targets the policy areas of identification, authentication, wireless application, encryption, dial–up access, access control, audit, firewalls, security incidents and violations, and preplanning and development initiatives.

Technical security issues and/or recommendations are addressed in the NCIC audit report and the CTO/FSC is given the opportunity to respond to any issues and/or recommendations. The CAU reports sanctionable offenses directly to the Advisory Policy Board (APB) Sanctions Subcommittee. The APB approved the CJIS Security Policy (August 2000), which specifies on page 13, "All FBI CJIS Division's data transmitted over dial-up or Internet connections shall be immediately protected with encryption. "All FBI CJIS Division's information passing through a public network segment must be protected with encryption, while in that segment with it sanctionable by close of fiscal year 2002, except for good cause shown to the APB, not to be extended past 2005."

The CAU presented the technical security audit methodologies at the ISO Training Symposium in Quantico, Virginia in the fall of 2000, disseminated the *CJIS Security Policy* to each CTA and incorporated the *CJIS Security Policy* as Section III of *A Policy and Reference Manual,* which is available on law Enforcement OnLine.

The technological advances that have presented themselves to the law enforcement community have also redefined the security risks that accompany implementation of such advances. As local, state, and federal agencies begin to implement security policies and requirements in the areas of dial-up access, Internet access, identification, authentication, and encryption, it is imperative that these agencies have a clear understanding of the importance of maintaining secure criminal justice information systems and networks; the threats, vulnerabilities, and risks faced by such systems and networks; and the appropriate countermeasures to address them. The CAU plays a role in ensuring the appropriate and effective implementation of technical policies by providing direct oversight at the local, state, and federal levels, thus ensuring the integrity and security of all CJIS systems and networks.

Agencies may contact the CJIS Division's ISP Mr. Steven Ahrens at: Contract Administration Office, CJIS Division, Federal Bureau of Investigations, 1000 Custer Hollow Road, Module C3, West VA 26306-0102;

Telephone 304-625-2763

Fax 304-625-3638

BMV Inquiries by Social Security Number

You have just made a BMV inquiry by Name and SOC, Name and OLN, or just by SOC, and you may have missed a "HIT" on the subject.

Why? When a BMV inquiry is made the information provided is used to search the following IDACS/NCIC files:

Wanted
Missing
Gang File
Protection Order (NCIC only)
Sexual Offender (NCIC 2000)
Supervised Release (NCIC 2000)
U.S. Secret Service Protective File

Because most entries do not contain the SOC or OLN of the subject entered, but are entered using the NAME and DATE OF BIRTH only.

What if the only information I have is the Name and OLN or SOC? Make the inquiry using the information you have. When information is returned from the BMV listing the Name and DOB of the subject another inquiry should be made using the Name and DOB.

REMEMBER TO CONFIRM ALL HITS BEFORE TAKING ANY ENFORCEMENT ACTION BASED ON THE INFORMATION RECEIVED FROM IDACS OR NCIC.

"Your transaction is a possible match with an Index Record"

Canadian Vehicle Index

In December 1998, the CJIS Advisory Policy Board approved the "pure" index design. This design allows for NCIC to continue to maintain the CVI. Instead of providing the CVI record in the response, NCIC will send a caveat informing the inquiring agency of a possible match with a Canadian Police Information Center (CPIC) record and that they may wish to query CPIC via National Law Enforcement Telecommunication System (NLETS). This method permits the agency to decide if the NLETS (CPIC) inquiry is necessary.

Caveat response

YOUR TRANSACTION IS A POSSIBLE MATCH WITH AN INDEX RECORD FOR A FELON VEHICLE IN CANADA WITH THE FOLLOWING IDENTIFIERS: ORI/ BCI1234567 VIN/ CAN1234567890 LICABC123 LIS/AB. ADDITIONAL INFORMATION MAY BE OBTAINED VIA NLETS USING A VQ OR XQ TRANSACTION. INTERNATIONAL USERS CONTACT INTERPOL OTTAWA.

Body Attachments

The entry of "Body Attachments" (civil warrants) into IDACS is not allowed. Current case law holds that law officers do not have the same authority to use force to gain entry to a residence when there is resistance, as they do to serve a criminal arrest warrant. Because of this and other factors, the IDACS Committee has voted not to allow entry of Body Attachments into the system. A complete copy of the legal opinion may be obtained by contacting the IDACS Section.

BMV Digital Picture Requests

Requests for an Indiana BMV digital picture and/or signature can be submitted to the Indiana State Police, GHQ, Operations Section. The requests may be submitted via switch message (INISP0005), in person, fax (317-232-0652) or by e-mail (opedl@isp.state.in.us). Requests submitted need the following information:

1. Subject's name and date of birth (exactly as it appears on the driver's license).
2. Subject's driver's license number.
3. Indiana BMV Transaction Number.
4. The Transaction Date
5. Requesting officer's last name and identification number.
6. Reason for request (example: case number, incident number, or UTT number)
7. A call back number, for any questions, concerning the request.

For quickest response it is recommended that your request be sent via e-mail.
Questions can be directed to the Operations Section at 317-232-8250

New IDACS Course

The new IDACS one-day "Update and Review" course is now being offered. The class is designed for experienced re-certifying operators who do not wish to attend the regular three day operator course or a test out. The course, plus the test will take six hours. New operators will not be scheduled for this course.

Administrative Tidbits

All IDACS sponsored training and testing begins at 8:30 a.m. local time for your area. IDACS monthly schedules for three day classes, one day update/review courses and test outs can be found in the IDACS help file (screen 015) INCALHELP.
Certified operators must be not more 180 days from their re-certification date before they can request attendance at an IDACS class, update/review or test out.
All coordinators must send a letter or switched message to IDACS when a last name needs to be changed, for example: marriage, etc. The request for a name change cannot be accepted at a IDACS class or test out.

Fingerprint Cards

In the future, the FBI will adapt a policy mandating the **REJECTION** of paper fingerprint cards that contain any **HIGHLIGHTED** areas. Contributors often use highlighter on paper cards to indicate fields that a applicant should complete i.e. Name, DOB, etc. The FBI's card scanning service cannot process fingerprint cards with highlighted areas. All agencies should take immediate action to stop this practice.

Violent Felon File

Notice anything missing from the NCIC Operating manual? The Violent Felon File has been eliminated.

Misuse of Distribution Codes & Training Messages

The IDACS Section has noticed that agencies are misusing the distribution codes to circumvent the "ALL STATIONS" policy. If this practice continues a "NOTICE OF VIOLATION" will be sent to the agency.
When the S0 codes are used to send an all stations some agencies will receive this message 3 or more times because they are in multiple distribution codes.

TRAINING MESSAGES
Agencies are placing the name of private vendors in the message. If this practice continues a "NOTICE OF VIOLATION" will be sent to the agency.

(Reprinted from the 1st Quarter 1997 IDACS News)

Place a copy of this information in the IDACS Manual Part IV Section B, "Message Switching Rules"

At the June 1996, meeting of the IDACS Committee the following rules for sending training messages was passed:

1. Send all training messages during the 12 AM – 6AM shift. This includes "All Station and Area Distribution Messages".

2. Continue the policy that the message be worded in such a way as not to mention private companies except as follows:
   a. Not for profit police/communications organizations i.e. APCO and National Emergency Number Association (NENA),
   b. Private companies that offer training on a specific piece of equipment software i. e. weapon armor's training (because it is of no value to an agency that does not use that weapon).

3. Continue to require the host agency to be responsible for furnishing additional information. The message must include the telephone number and a contact person for the host agency.

4. Schedule for transmitting of training message:

   a. Initial message 60 days prior to the training
   b. Interim message 30 days prior to the training
   c. Final message 2 weeks prior to the training

The message must include whether this is the "Initial", "Interim", or "Final" message.

Place a copy of this in the IDACS Manual, Part IV, and Section B – MESSAGE SWITCHING - RULES
IDACS Committee
(Reprinted from the 1st Quarter 1998 IDACS News)

Expiration Period for New Terminal Requests/ MDD's Or Additional Terminals

Any approval granted by the IDACS Committee for the following actions is valid for twelve (12) months from the approval date:

- Approval to become a terminal agency
- Approval to add additional terminals which include Mobile Data Devices

If the approved action is not completed within this time frame, another request will need to be submitted.

IDACS welcomes two (2) new members to the IDACS staff. Kelly Dignin who will be the IDACS instructor for the northwest area of the state and Ala Munn our new clerical assistant.

IDACS

Indiana Government Center North
100 North Senate Ave.
Indianapolis, IN 46204-2259

Phone: 317.232.8292
Fax: 317.233.8323

Vivian Nowaczewski Editor and Chief
Kelly Dignin Assistant Editor and Chief

IDACS Staff

Program Director
Andre' Clark

IDACS System Coordinator
Michael Dearinger

Administration
Ala Munn
Holly White

IDACS Security
Sgt. John Clawson
Sgt. John Richards

IDACS Training
Kelly Dignin
Larry McRae
Vivian Nowaczewski
Troy Scott

Information Security Officer (ISO)
Dennis Eaton

Data Operations Center Staff

Supervisor
Carrie Hampton

Day Shift (0700-1500)
Eric R. Macy (working leader)
LaJuan Harris
Tamara Whatley

Evening Shift (1500-2300)
Patricia Cork (working leader)
Patsity Epps
Leldo Ba

Night Shift (2300-0700)
Jasmine O. Munn (working leader)
Brian Thayer
Wayne Eric Swift